International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 9/32

A1

(11) International Publication Number: WO 00/54457

(43) International Publication Date: 14 September 2000 (14.09.00)

(21) International Application Number: PCT/FI00/00176

(22) International Filing Date: 7 March 2000 (07.03.00)

(30) Priority Data:
990502 8 March 1999 (08.03.99) FI

(71) Applicant *(for all designated States except US)*: SONERA SMARTTRUST OY [FI/FI]; c/o Sonera OY, P.O.box 106, FIN-00051 Sonera (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: VATANEN, Harri [FI/GB]; 2 Rushmere Place, Englefield Green, Surrey TW20 0NN (GB).

(74) Agent: PAPULA OY; P.O. Box 981 (Fredrikinkatu 61 A), FIN-00101 Helsinki (FI).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

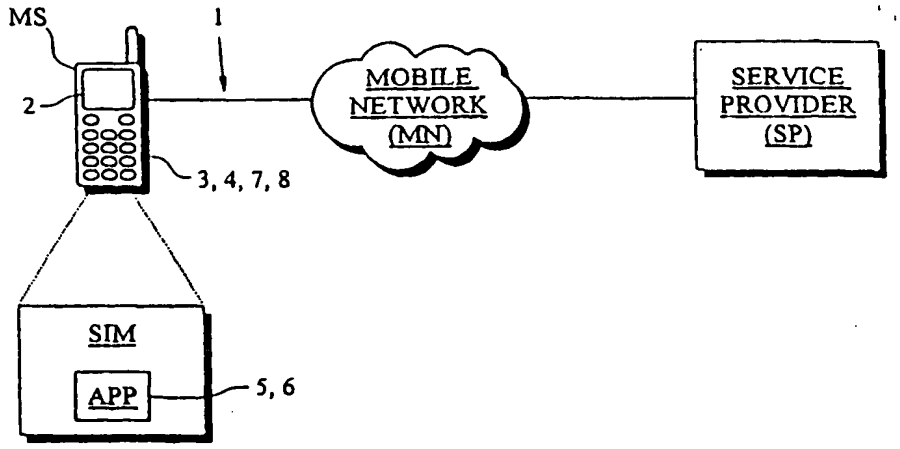
Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

In English translation (filed in Finnish).

(54) Title: METHOD AND SYSTEM IN A TELECOMMUNICATION SYSTEM



(57) Abstract

System, method and mobile station for implementing a secure transaction. The system comprises a mobile communication network (MN), a service provider (SP) communicating with the mobile communication network, a mobile station (MS) communicating with the mobile communication network (MN) and via it with the service provider (SP), said mobile station (MS) comprising a subscriber identity module (SIM), and a service application (APP) stored in the subscriber identity module (SIM), said mobile station (MS) communicating with the service provider (SP) over the mobile communication network (MN). The system further comprises means (1) for transferring the material needed in the transaction into the mobile station (1), and means (1) in the mobile station (MS) for presenting the material to the user. According to the invention, the system further comprises means (3) for requesting the user's acceptance of the material for signature, means (4) for activating a PIN inquiry if the user accepts the material, means (5) for checking the correctness of the PIN code entered by the user in the subscriber identity module, and means (6) for encrypting and/or signing the material using the service application stored in the subscriber identity module if the PIN code entered by the user is correct.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PC

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD AND SYSTEM IN A TELECOMMUNICATION SYSTEM

The present invention relates to telecommunication systems. In particular, the invention concerns an advanced method and system of a new type that allows the receiver of a service to safely and flexibly accept the material needed in a transaction via his/her mobile station.

BACKGROUND OF THE INVENTION

In prior art, a known practice is to use a digital mobile station in a communication system, such as the GSM system (Global System for Mobile communications, GSM), for commercial transactions, such as paying a bill or remitting a payment, by electronic means. Patent specification US 5,221,838 presents a device which can be used for making a payment. The specification describes an electronic payment system in which a terminal capable of wireless and/or wired data transfer is used as a payment terminal. The terminal described in the specification comprises a card reader, a keyboard, a bar code reader for data input and a display for presentation of payment information.

Patent specification WO 94/11849 presents a method for utilization of telecommunication services and for performing payment transfers via a mobile telephone system. The specification describes a system comprising a terminal which communicates over a telecommunication network with a service provider's mainframe computer containing the service provider's payment system. A terminal in the mobile telephone network, i.e. a mobile station, can be provided with a subscriber identity unit which contains information required for subscriber identification and encryption of telecommunication traffic. The information can be read into the terminal for use in mobile stations. As an example, the specification mentions the GSM system,

in which a SIM card (Subscriber Identity Module, SIM) is used as a subscriber identity unit.

In the system described in specification WO 94/11849, the mobile station communicates with a base transceiver station in the mobile communication network. According to the specification, a connection is set up from the base transceiver station further to a payment system and the amount to be paid as well as the data required for subscriber identification are transmitted to the payment system. In the bank service described in the specification, the client inserts a bank service card containing a SIM unit into a GSM network terminal. In the telephone based bank service, the terminal may be a standard GSM mobile station. Using the method described in the specification it is possible to use a wireless telecommunication connection for remitting payments and/or paying bills or implementing other corresponding bank services.

A problem in the prior-art solutions is that they do not pay attention to the reliability of a payment transaction carried out by means of a mobile station. It is important that the application in the mobile station which makes the payment transaction possible should verify the user's authenticity separately for each transaction. When a mobile station is used for remitting a payment, it is important that both the payer and the payee can rely on the system. The payer needs to know exactly what he is paying for, how much he is paying, to whom he is paying, and so on. On the other hand, the receiver of the payment needs to know with certainty that the payer has expressed his will for the remittance of the payment.

Digital signature, which is considered a general requirement in electronic payment, is used for verification of the integrity of the material transmitted and the authenticity of the sender. A digital signature is generated by encrypting a hash code com-

puted from the material to be transmitted, using the sender's secret key. Since nobody else knows the sender's secret key, the receiver, when decrypting the information using the sender's public key, can ascertain that the material is unchanged and that it has been generated by the sender. An example of the algorithm used in digital signature is the RSA encryption algorithm, which is a public and private key encryption system and which is also used for the encryption of messages.

OBJECT OF THE INVENTION

The object of the present invention is to eliminate the problems described above or at least to alleviate them. A specific object of the invention is to disclose a new type of method and system for accepting material needed in a transaction separately for each transaction. In this context, 'material' may refer to many types of electronically interpretable message, notice or data structure of various contents. The material may consist of object type or software object type information which can be processed in an electronic form.

A further object of the invention is to disclose a simple method for implementing commercial transactions, such as paying bills and banking, by means of a mobile station, a method that can be easily implemented with modern technology.

SUBJECT OF THE INVENTION

The invention concerns a method for implementing a secure transaction by means of a mobile station which comprises a subscriber identity module and a service application stored in the subscriber identity module. The mobile station communicates with a service provider via a mobile communication network.

The mobile communication network may be a GSM network. In the method, the material needed in the transaction is transferred into the mobile station and the material is presented by means of the mobile station. After that, according to the invention, the user is asked to give his/her approval for signature of the material, a PIN inquiry is activated in the mobile station if the user accepts the material, the PIN code entered by the user is checked for correctness in the subscriber identity module, and, if the PIN code given by the user is correct, the material is encrypted and/or signed using the service application stored in the subscriber identity module.

In an embodiment of the invention, if the user of the mobile station does not accept the material needed in the transaction for signature or if three successive entries of the user's PIN code are incorrect, then a reject message is sent to the service provider having generated the material. The material can be generated using a pre-agreed form overlay in which the essential information is filled in before its being transferred into the mobile station, or using some other mutually agreed and known data structure.

In the foregoing, a procedure has been described in which the client accepts the material he/she sees on the display of the mobile station, which material, after being accepted, is sent to the service provider, such as a bank. The client or mobile station user may communicate locally with an automatic payment machine or equivalent, in which case the payment machine transmits to the client the material intended to be accepted. In this case, the client exchanges messages locally with the payment machine and the payment machine transmits the digital signature information further. The local communication can be

performed without necessarily using a mobile communication network.

From the payment traffic it is handling, the payment machine can infer that the client has accepted the service and payment form presented. Thus, the machine can serve the client locally in the manner desired and approved by the client, without necessarily expecting the bank's approval for it. In practice, the situation corresponds to the normal practice when a client pays for products or services using his/her bank card e.g. at a cash desk in a store and the store provides the products/services to the client without contacting the bank to verify the authenticity of the payment.

The material may also be encrypted before being transferred into the mobile station, in which case the material has to be decrypted before being signed. In this way, it is possible to make sure that only the intended mobile station will receive the material transmitted and to guarantee security of the information.

In one embodiment, the mobile station may be required to be started in signature mode before the material is transferred into it. In practice, this may mean that the user has to enter another predetermined PIN code with which the mobile station has been configured to start in a predetermined signature mode. Thus, a kind of local authentication can be used.

The invention also concerns a system for implementing a secure transaction using a mobile station, said system comprising a mobile communication network, a service provider communicating with the mobile communication network, and a mobile station communicating with the mobile communication network and over the network with the service provider. The mobile station comprises a subscriber identity module and a service application stored in the subscriber identity

module. The mobile station preferably communicates with the service provider via the mobile communication network. The system additionally comprises means for transferring the material needed in the transaction into the mobile station. These means may be implemented in the mobile communication network and in the mobile station e.g. using a short message service or using a local link, e.g. an infrared link or a Bluetooth link. A more detailed description of the Bluetooth technology is presented e.g. on WWW page www.bluetooth.com. In addition, the mobile station comprises means, such as a display, for presenting the material to the user.

According to the invention, the system comprises means for requesting the user's acceptance of the material, means for activating a PIN inquiry if the user accepts the material, means for verifying the PIN code supplied by the user in the subscriber identity module, and means for encrypting and/or signing the material using the service application stored in the subscriber identity module if the PIN code given by the user is correct.

Moreover, the system may further comprise means for sending a reject message to the service provider having generated the material if the user of the mobile station does not accept the material needed in the transaction for signature or if the PIN code input into the mobile station is incorrect.

As compared with prior art, the invention has the advantage that it makes it easier to implement payment applications, verification operations and the like using a mobile station while at the same time providing a higher level of security for the users. The invention allows reliable use of a mobile station for accepting material needed in a transaction and for signing it digitally, allowing acceptance and digital

signature to be applied in conjunction with many different applications.

LIST OF ILLUSTRATIONS

In the following, the invention will be described by the aid of preferred examples of its embodiments with reference to the attached drawing, wherein:

Fig. 1 presents a preferred system according to the present invention;

Fig. 2 presents a diagram of a preferred arrangement according to the present invention; and

Fig. 3 presents a diagram representing a preferred embodiment of the present invention.

The system presented in Fig. 1 comprises a mobile communication network, a mobile station MS connected to it and a service provider SP. The mobile communication network may be e.g. a GSM network. The service provider may be a store, a bank, a parking facility, a ticket office or any corresponding service provider. In practice, the service provider is connected to the mobile communication network via a terminal or server resembling a mobile station or via a combination of these. However, it will not be described here in detail because there are various devices obvious to the skilled person that the service provider can use as a link to the mobile communication network.

The mobile station comprises a subscriber identity module SIM with a service application APP stored in it, said service application implementing the transaction at the mobile station end in cooperation with the service provider, and a display 2 for presenting the material to the user. Stored in the service application are also the encryption and decryption keys needed in the transaction. In addition, the service application has information regarding

other parameters and data structures used in the service.

The mobile station presented in Fig. 1 further comprises means 3 for requesting the user's acceptance of the material, means 4 for activating a PIN inquiry if the user accepts the material, means 5 for checking the PIN code supplied by the user for correctness in the subscriber identity module, and means 6 for encrypting and/or signing the material using the service application stored in the subscriber identity module if the PIN code given by the user is correct. Means 3, 4, 5 and 6 may be implemented in a suitable component in the mobile station or in the subscriber identity module, or some of them may be implemented as separate components in the mobile station and in the subscriber identity module. In system presented in this figure, the PIN code is checked for correctness in the subscriber identity module using means 5 and the material is also encrypted and/or signed in the subscriber identity module using means 6.

The system illustrated in Fig. 1 further comprises means for sending a reject message to the service provider having generated the material if the user of the mobile station does not consent to sign the material needed in the transaction. The corresponding system comprises means 8 for sending a reject message to the service provider having generated the material if the PIN code entered into the mobile station is incorrect. This alternative is optional, and the message can be sent e.g. when incorrect entries are to be recorded in the system. In practice, this can be implemented by sending a message to the service provider after the user has entered an incorrect PIN code e.g. three times. The service provider can then take measures to establish the authenticity of the user of the mobile station.

Fig. 2 presents a diagram visualizing an embodiment of the present invention. In the figure, the material DATA to be signed has been printed on the display of the mobile station 2, and the user may either accept or reject it. When the user presses the Accept button to indicate that he/she accepts the material DATA, the user's choice triggers the next action in the procedure. The text "PIN:?" appears on the display, asking the user to give a transaction-specific PIN code. After the user has keyed in a correct PIN code, the service application APP (Fig. 1) performs the required operations on the material and sends it to the service provider SP together with an accept message. If the user rejects the data, then a reject message is sent to the service provider.

Fig. 3 presents a flow diagram representing a preferred embodiment of the invention. First, the material is transferred into the mobile station, block 31. In the mobile station, the material is presented e.g. on the display 2 (see Fig. 1), block 32. At the same time, the user is asked whether he/she will accept or reject the material, block 33. If the user accepts the material, then the procedure goes on to block 35, where the required actions for encrypting and/or signing the material are performed. After that, the material together with an accept message is sent to the service provider, block 36. If in block 33 the user rejects the material, then the procedure goes on to block 34 and a reject message is sent to the service provider.

To sum up, it can be stated that the invention significantly facilitates the operations to be carried out by a mobile station user in conjunction with a transaction made via a mobile station. The invention also improves the security of transactions made via a mobile station. In practice, the encrypting and signing procedures needed in the method of the in-

vention are based on an application which is stored in the subscriber identity module and/or mobile station e.g. in a digital signal processor and which performs the required operations on the material after the user has accepted it. The material can be transmitted into the mobile station on the basis of an order made e.g. by telephone or over the Internet, in which case the acceptance of the material functions as a kind of acknowledgement to the service provider with whom the order was placed. Accepting the material may constitute an acknowledgement and approval of an order, offer, parking charge or any relevant service involving a transaction.

The present invention is not restricted to the examples of its embodiments described above; instead, many variations are possible within the sphere of protection defined in the claims.

CLAIMS

1. Method for implementing a secure transaction using a mobile station comprising:

a subscriber identity module,

a service application stored in the subscriber identity module, said mobile station communicating with a service provider over a mobile communication network,

said method comprising the steps of:

transferring the material needed in the transaction into the mobile station, and

presenting the material on the mobile station, characterized in that the method further comprises the steps of:

requesting the user's acceptance of the material,

activating a PIN inquiry if the user accepts the material,

checking the PIN code entered by the user for correctness in the subscriber identity module, and

encrypting and/or signing the material using the service application stored in the subscriber identity module if the PIN code given by the user is correct.

2. Method as defined in claim 1, characterized in that

a reject message is sent to the service provider having generated the material if the user of the mobile station does not accept the material needed in the transaction for signature.

3. Method as defined in claim 1, characterized in that

a reject message is sent to the service provider having generated the material if the PIN code input into the mobile station is incorrect.

4. Method as defined in any one of the preceding claims 1, 2 or 3, characterized in that

the material is composed using a pre-agreed form overlay provided with an identifier, in which the essential information is filled in before its being transferred into the mobile station.

5. Method as defined in any one of the preceding claims 1, 2, 3, or 4, characterized in that

the mobile station is started in signature mode before the material is transferred into the mobile station.

6. Method as defined in any one of the preceding claims 1, 2, 3, 4 or 5, characterized in that

the message is signed and/or encrypted using a public and private key method.

7. System for implementing a secure transaction using a mobile station, said system comprising:

a mobile communication network (MN),

a service provider (SP) communicating with the mobile communication network,

a mobile station (MS) communicating with the mobile communication network (MN) and via the network with the service provider (SP), said mobile station (MS) comprising:

a subscriber identity module (SIM), and

a service application (APP) stored in the subscriber identity module (SIM) and a mobile station (MS) communicating with the service provider (SP) over the mobile communication network (MN).

means (1) for transferring the material needed in the transaction into the mobile station (1), and

means (2) in the mobile station (MS) for presenting the material, characterized in that the system further comprises:

means (3) for requesting the user's acceptance of the material,

means (4) for activating a PIN inquiry if the user accepts the material,

means (5) for checking the PIN code entered by the user for correctness in the subscriber identity module, and

means (6) for encrypting and/or signing the material using the service application stored in the subscriber identity module if the PIN code entered by the user is correct.

8. System as defined in claim 7, characterized in that the system further comprises:

means (7) for sending a reject message to the service provider having generated the material if the user of the mobile station does not accept the material needed in the transaction for signature.

9. System as defined in claim 7, characterized in that the system further comprises:

means (8) for sending a reject message to the service provider having generated the material if the PIN code entered into the mobile station is incorrect.

10. System as defined in any one of the preceding claims 7, 8 or 9, characterized in that

a pre-agreed form overlay provided with an identifier has been stored in the subscriber identity module, in which form overlay the essential information is filled in and which is used for presenting the material to the user.

11. Mobile station for implementing a secure transaction, said mobile station (MS) comprising:

a subscriber identity module (SIM), and

a service application (APP) stored in the subscriber identity module SIM,

means (1) for receiving the material needed in the transaction into the mobile station (1), and

means (2) for presenting the material, characterized in that the mobile station further comprises:

means (3) for requesting the user's acceptance of the material,

means (4) for activating a PIN inquiry if the user accepts the material,

means (5) for checking the PIN code entered by the user for correctness in the subscriber identity module, and

means (6) for encrypting and/or signing the material using the service application stored in the subscriber identity module if the PIN code entered by the user is correct.

12. Mobile station as defined in claim 11, characterized in that the mobile station further comprises:

means (7) for sending a reject message to the service provider having generated the material if the user of the mobile station does not accept the material needed in the transaction for signature.

13. Mobile station as defined in claim 11, characterized in that the system further comprises:

means (8) for sending a reject message to the service provider having generated the material if the PIN code input into the mobile station is incorrect.

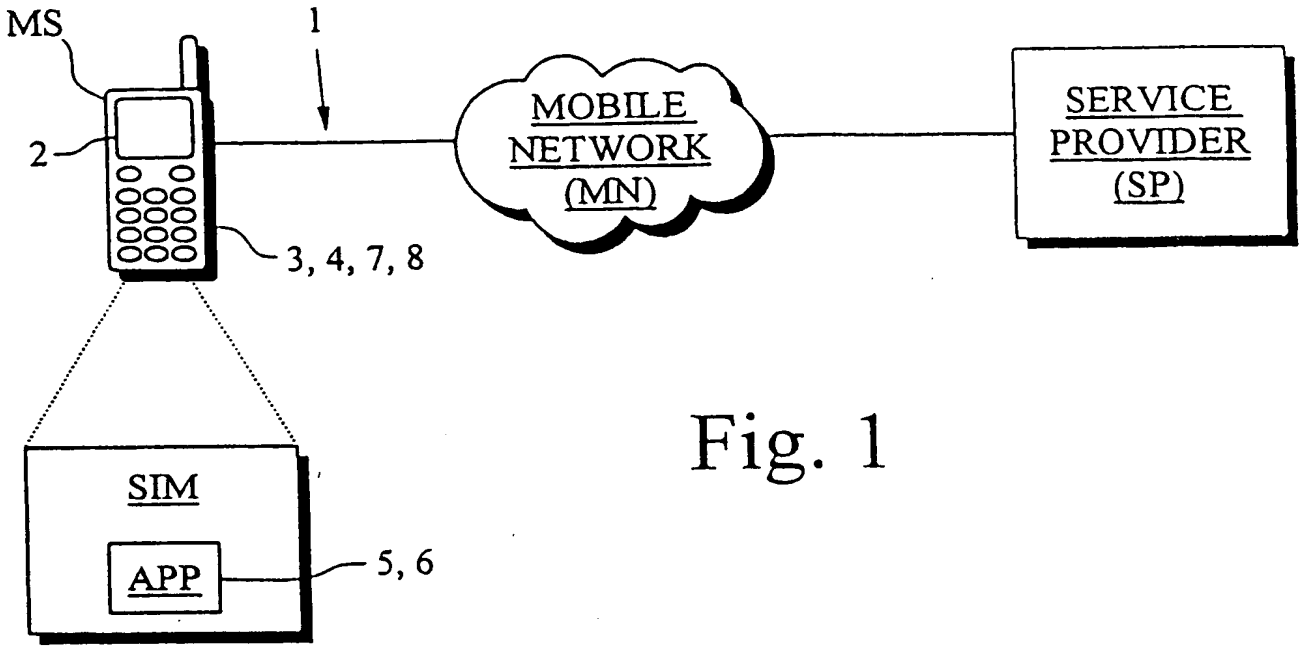

MS
1
2
MOBILE NETWORK (MN)
SERVICE PROVIDER (SP)
3, 4, 7, 8
SIM
APP
5, 6

Fig. 1

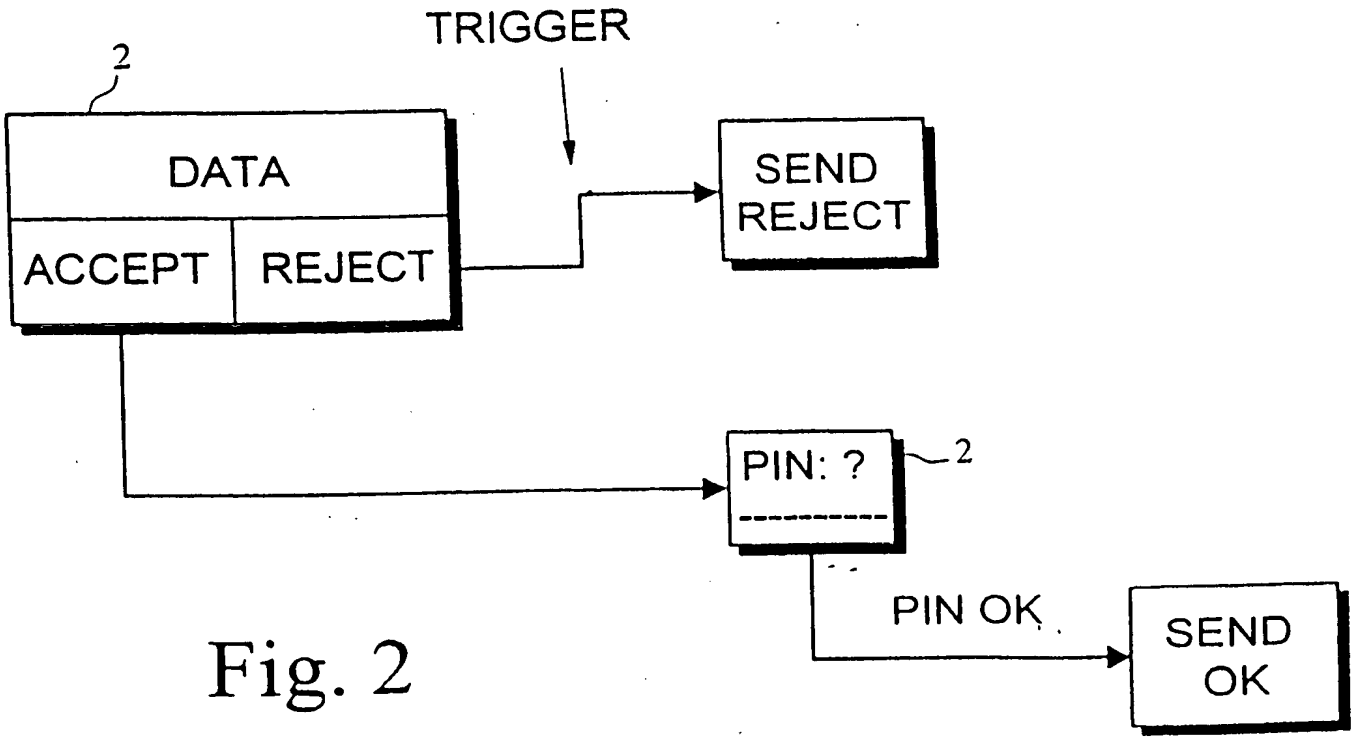

TRIGGER
2
DATA
ACCEPT
REJECT
SEND REJECT
PIN: ?
2
PIN OK
SEND OK

Fig. 2

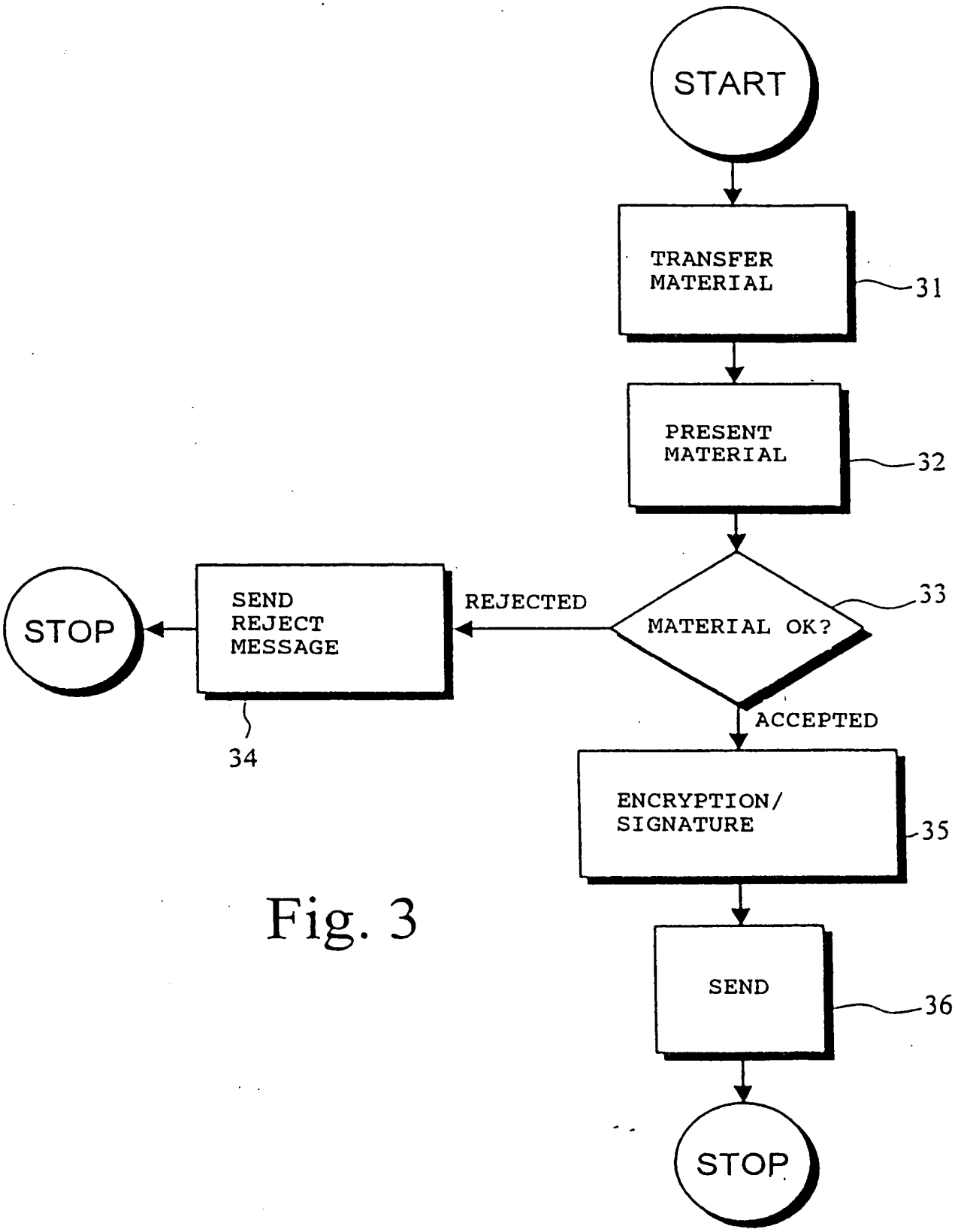

START
TRANSFER MATERIAL
31
PRESENT MATERIAL
32
MATERIAL OK?
33
REJECTED
SEND REJECT MESSAGE
STOP
34
ACCEPTED
ENCRYPTION/ SIGNATURE
35
SEND
36
STOP

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/00176

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04M, H04L, G07F, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9837663 A1 (POSTGIROT BANK AB), 27 August 1998 (27.08.98), page 5, line 18 - line 22; page 5, line 35 - page 6, line 17; page 6, line 26 - line 36, page 7, line 15 - line 21	1-13
A	EP 0785534 A1 (KONINKLIJKE PTT NEDERLAND N.V.), 23 July 1997 (23.07.97), column 2, line 14 - line 30	1-13

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 July 2000	27 -07- 2000
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson/AE Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/FI 00/00176

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9837663 A1	27/08/98	AU 2983797 A	30/10/98
		AU 6126898 A	09/09/98
		NO 993939 D	00/00/00
		SE 507062 C	23/03/98
		SE 508844 C	09/11/98
		SE 9503498 A	10/04/97
		SE 9700587 A	20/08/98
		WO 9845101 A	15/10/98
EP 0785534 A1	23/07/97	NONE	